



IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Inventors: Y. YOKOMITSU, et al.

Application No.: 10/827,371

Filed: April 20, 2004

For: A REPEATER AND AN INTER-NETWORK REPEATING METHOD

CLAIM FOR PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified application and the priority provided in 35 USC 119 is hereby claimed:

Japanese Appln. No. 2003-115568, filed April 21, 2003.

In support of this claim, a certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 USC 119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

James E. Ledbetter
Registration No. 28,732

Date: June 16, 2004

JEL/spp
Attorney Docket No. L8612.04111
STEVENS, DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, NW, Suite 850
P.O. Box 34387
Washington, DC 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2003年 4月21日

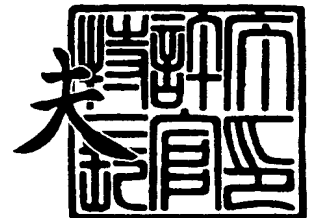
出願番号
Application Number: 特願2003-115568
[ST. 10/C]: [JP2003-115568]

出願人
Applicant(s): 松下電器産業株式会社

2004年 4月12日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2004-3030094

【書類名】 特許願

【整理番号】 2913050136

【提出日】 平成15年 4月21日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 29/12

【発明者】

【住所又は居所】 福岡市博多区美野島4丁目1番62号 パナソニック
コミュニケーションズ株式会社内

【氏名】 横光 康志

【発明者】

【住所又は居所】 福岡市博多区美野島4丁目1番62号 パナソニック
コミュニケーションズ株式会社内

【氏名】 八尾 昭男

【発明者】

【住所又は居所】 福岡市博多区美野島4丁目1番62号 パナソニック
コミュニケーションズ株式会社内

【氏名】 濱▲崎▼ 敏幸

【発明者】

【住所又は居所】 福岡市博多区美野島4丁目1番62号 パナソニック
コミュニケーションズ株式会社内

【氏名】 小西 宏

【発明者】

【住所又は居所】 福岡市博多区美野島4丁目1番62号 パナソニック
コミュニケーションズ株式会社内

【氏名】 執行 正浩

【発明者】

【住所又は居所】 福岡市博多区美野島4丁目1番62号 パナソニック
コミュニケーションズ株式会社内

【氏名】 満永 雄二

【発明者】

【住所又は居所】 福岡市博多区美野島 4 丁目 1 番 6 2 号 パナソニック
コミュニケーションズ株式会社内

【氏名】 鷺谷 公憲

【発明者】

【住所又は居所】 福岡市博多区美野島 4 丁目 1 番 6 2 号 パナソニック
コミュニケーションズ株式会社内

【氏名】 長尾 英明

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 中継装置

【特許請求の範囲】

【請求項 1】 第 1 ネットワークと第 2 ネットワークとの間の通信パケットの中継を行う中継装置であって、

前記第 1 ネットワーク側の外部ポート番号が前記第 2 ネットワーク側に接続された端末装置の内部 I P アドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、

前記外部ポート番号を指定した通信パケットを受信すると、前記ポートマッピングテーブルに基づいて前記内部ポート番号に変換して前記第 2 ネットワークに転送する制御手段と、

前記内部ポートに変換した通信パケットを転送してからの該ポートの未使用時間を計時するタイマ手段と、

前記ポートの未使用時間が所定時間になると、前記ポートマッピングテーブルから前記外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置。

【請求項 2】 前記未使用時間が、前記第 2 ネットワークに接続された端末装置からのアクセスにより、ユーザが設定可能であることを特徴とする請求項 1 記載の中継装置。

【請求項 3】 前記ポート管理手段が、ポートが開かれている時間をモニタして最長時間を記録し、該最長時間以上の時間を前記未使用時間の閾値として設定することを特徴とする請求項 1 または 2 記載の中継装置。

【請求項 4】 第 1 ネットワークと第 2 ネットワークとの間の通信パケットの中継を行う中継装置であって、

前記第 1 ネットワーク側の外部ポート番号が前記第 2 ネットワーク側に接続された端末装置の内部 I P アドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、

前記外部ポート番号を指定した通信パケットを受信すると、前記ポートマッピングテーブルに基づいて前記内部ポート番号に変換して前記第 2 ネットワークに

転送する制御手段と、

前記内部ポートに変換した通信パケットを転送してからの該ポートの未使用時間を計時するタイマ手段と、

通信パケットを所定時間受信していないと判断した場合には、前記第 2 ネットワークに接続された端末装置に存在確認のパケットを送信し、応答がない場合に前記ポートマッピングテーブルから前記前記外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置。

【請求項 5】第 1 ネットワークと第 2 ネットワークとの間の通信パケットの中継を行う中継装置であって、

前記第 1 ネットワーク側の外部ポート番号が前記第 2 ネットワーク側に接続された端末装置の内部 I P アドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、

前記外部ポート番号を指定した通信パケットを受信すると、前記ポートマッピングテーブルに基づいて前記内部ポート番号に変換して前記第 2 ネットワークに転送する制御手段と、

前記第 2 ネットワーク側に接続された端末装置に存在確認のパケットを定期的に送信するための時間を計時するタイマ手段と、

前記タイマ手段が計時した時刻に前記第 2 ネットワークに接続された端末装置に存在確認のパケットを送信し、応答がない場合に前記ポートマッピングテーブルから前記前記外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置。

【請求項 6】前記ポート管理手段が、前記第 2 ネットワークに接続された端末からの要求に基づいて前記ポートマッピングテーブルへの登録を行うことを特徴とする請求項 1 ～ 5 のいずれかに記載の中継装置。

【請求項 7】中継装置が、U P n P 規格に従って I P パケットを動的にポートフォワーディングするルータであることを特徴とする請求項 1 ～ 6 のいずれかに記載の中継装置。

【請求項 8】第 1 ネットワークと第 2 ネットワークとの間の通信パケットの中継を行う中継装置であって、

前記第 1 ネットワーク側の外部ポート番号が前記第 2 ネットワーク側に接続された端末装置の内部 IP アドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、

前記外部ポート番号を指定した通信パケットを受信すると、前記ポートマッピングテーブルに基づいて前記内部ポート番号に変換して前記第 2 ネットワークに転送する制御手段と、

DHCP リース期限に再リースをするか否かを確認し、前記端末装置からの再リース要求を受信する DHCP サーバ部と、

前記端末装置からの再リース要求がなかった場合には、前記ポートマッピングテーブルから前記前記外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ルータなどの中継装置に関し、とくに動的にポートフォワーディング設定を行ってポートを開設するとともに、この動的に開かれたポートを自動的に閉鎖する中継装置に関するものである。

【0002】

【従来の技術】

インターネット等の広域ネットワークへ常時接続するため ADSL, CATV の普及が本格化し、ブロードバンドルータの普及も著しい。しかし、現行の IP プロトコル IPv4 ではグローバル IP アドレス（以下、外部 IP アドレス）の絶対数が不足しているため、NAT (Network Address Translation) 機能やポートフォワーディング機能（静的 IP マスカレード）などを使用して外部 IP アドレスの不足に対応している。この NAT 機能は、LAN 側の機器からインターネットへアクセスするときには、そのローカル IP アドレス（内部 IP アドレス、以下、IP アドレスという）をルータの WAN 側の外部 IP アドレスへ変換するものである。

【0003】

インターネットからLAN側の特定の機器へアクセスする場合、ルータのポートフォワーディング機能（静的IPマスカレード機能）を用いることでアクセスが可能になる。すなわち、これにはまず予め、ルータにポート番号とIPアドレスの変換テーブルを設定しておき、インターネットからアクセスするときには、ルータの外部IPアドレスと外部ポート番号を指定する。このアクセスを受け付けたルータは予め設定された変換テーブルに従い、外部IPアドレスをIPアドレスに変換する。この変換によりIPアドレスをもったLAN内の機器にアクセスすることが可能となる。

【0004】

このポートフォワーディング機能、NAT機能により従来のルータは、外部IPアドレスの枯渇を緩和し、LAN内の複数のユーザ機器とインターネットとを接続したが、ユーザは機器のポート番号を得て、その設定や変更を手動で行う必要があった。

【0005】

しかし、手動での設定は煩わしい上に、ポートの活用という点では不十分でもあるため、UPnPフォーラムにより、動的にポートフォワーディング設定（ポートマッピング）を行う規格が作成された（非特許文献1参照）。この規格の設定は、配下の端末からルータに対してポートを開設するように要求し、ルータはそれが可能な場合には登録し、使用不可の場合には端末は再度要求し、決定するまでこれを繰り返すものである。なお、UPnP規格ではポートは無期限もしくは有期限で割り当てることができ、この有期限の割り当てを利用すれば、ルータのベンダーによらず動的に設定した外部ポートを自動的に削除させることができる。図12は従来の動的ポートフォワーディングにおけるポート割当からポート解除までのシーケンスチャートである。

【0006】

図12に示すように、外部IPアドレス「232.0.0.1」（DHCPサーバによって割り当てられたIPアドレス「192.168.0.4」）のルータにLAN内の内部ポート番号「8080」がユーザ設定されたサーバAを接続すると、サーバAはDHCP発見パケットを送信し、DHCPサーバがIPアド

レス「192.168.0.1」を割り当てる。続いてサーバAはルータ発見パケットを送信し（sq101）、ルータがこれに対して応答する（sq102）。これを受信するとサーバAはポート登録要求を送信し（sq103）、ルータは外部ポート番号「80」を割り当てて応答する（sq104）。

【0007】

その後、インターネットに接続された外部IPアドレス「232.0.0.2」のクライアント端末からサーバAに「http://232.0.0.1:80」でアクセスすると（sq105）、ルータは「http://192.168.0.1:8080」にポートフォワーディングする（sq106）。サーバAはこれに対してレスポンスを返し（sq107）、クライアント端末はサーバAの処理を求めてアクセスし（sq108）、サーバAはレスポンスを送信する（sq109）。その後、クライアント端末とサーバAとの間で通信が終了する。その後、ポートの割当てがサーバAからの無期限の割当て要求によるものである場合、通信が終了しているにも関わらず、ポートはサーバAに割当てられたままとなる。

【0008】

【非特許文献1】

UPnP規格、[online]、[平成15年1月13日検索]、インターネット<URL:http://www.upnp.org/standardizeddcp/default.asp>

【0009】

【発明が解決しようとする課題】

以上説明したように従来のルータのポートフォワーディング機能（静的IPマスカレード機能）は、LAN側の端末装置に対して外部ポート番号を用いてアクセスできるものである。しかし、LAN側のシステム変更に伴って外部ポート番号に変更が発生した場合、その変更をすべて手動で設定し直さなければならなかった。

【0010】

また、UPnPフォーラムの規格によって動的にポートフォワーディング設定

した場合、ポートの割当てがサーバや端末からの無期限の割当て要求によるものである場合、通信が終了しているにも関わらず、ポートはサーバや端末に割当てられたままとなる。従って、サーバの電源がOFFとなった場合や、通信していた端末のアプリケーションが終了した場合には、そのポートが使用されないのにも関わらず、残ったままとなり、このポートがセキュリティホールとなって不正アクセスを許す可能性があった。

【0011】

そこで本発明は、動的に開かれたポートを設定に従って自動的に閉じる中継装置を提供することを目的とする。

【0012】

【課題を解決するための手段】

上記の課題を解決するために本発明は、第1ネットワークと第2ネットワークとの間の通信パケットの中継を行う中継装置であって、第1ネットワーク側のグローバルIPアドレスと外部ポート番号が第2ネットワーク側に接続された端末装置のローカルIPアドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、外部ポート番号を指定した通信パケットを受信すると、ポートマッピングテーブルに基づいて内部ポート番号に変換して第2ネットワークに転送する制御手段と、内部ポートに変換した通信パケットを転送してからの該ポートの未使用時間を計時するタイマ手段と、ポートの未使用時間が所定時間になると、ポートマッピングテーブルから外部ポート番号に関する登録を削除するポート管理手段を備えたものである。

【0013】

これにより、動的に開かれたポートを設定に従って自動的に閉じることができる。

【0014】

【発明の実施の形態】

本発明の請求項1は、第1ネットワークと第2ネットワークとの間の通信パケットの中継を行う中継装置であって、第1ネットワーク側の外部ポート番号が第2ネットワーク側に接続された端末装置の内部IPアドレスと内部ポート番号に

関係付けられたポートマッピングテーブルと、外部ポート番号を指定した通信パケットを受信すると、ポートマッピングテーブルに基づいて内部ポート番号に変換して第 2 ネットワークに転送する制御手段と、内部ポートに変換した通信パケットを転送してからの該ポートの未使用時間を計時するタイマ手段と、ポートの未使用時間が所定時間になると、ポートマッピングテーブルから外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置であり、ポートの未使用時間が所定時間を超えたとき、ポート管理手段によってポートを閉鎖するから、ポートが開かれたままでは不正アクセスされる危険があるが、所定時間以上経過するとポートは閉鎖され、これによって端末装置内部の情報が漏れることはない。

【0 0 1 5】

本発明の請求項 2 は、未使用時間が、第 2 ネットワークに接続された端末装置からのアクセスにより、ユーザが設定可能であることを特徴とする請求項 1 記載の中継装置であり、ポートを閉鎖するための時間はユーザによってまちまちであるが、ユーザが中継装置にアクセスしてこの時間を任意に設定できるから、手軽に個人個人で最も希望に適ったポート閉鎖を行うことができる。

【0 0 1 6】

本発明の請求項 3 は、ポート管理手段が、ポートが開かれている時間をモニタして最長時間を記録し、該最長時間以上の時間を未使用時間の閾値として設定することを特徴とする請求項 1 または 2 記載の中継装置であり、ポートを開いて閉じるまでの時間の利用実態を考慮し、過去の利用の中で最大時間を記憶するので、次の要求に対しては前回利用時間より大きい時間を設定すれば、利用中にも関わらずポートを閉鎖する可能性が低くなり、一方ポートが開いているにもかかわらず利用されていない期間が存在する確率を最小限にすることが可能となる。

【0 0 1 7】

本発明の請求項 4 は、第 1 ネットワークと第 2 ネットワークとの間の通信パケットの中継を行う中継装置であって、第 1 ネットワーク側の外部ポート番号が第 2 ネットワーク側に接続された端末装置の内部 IP アドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、外部ポート番号を指定した通信パ

ケットを受信すると、ポートマッピングテーブルに基づいて内部ポート番号に変換して第2ネットワークに転送する制御手段と、内部ポートに変換した通信パケットを転送してからの該ポートの未使用時間を計時するタイマ手段と、通信パケットを所定時間受信していないと判断した場合には、第2ネットワークに接続された端末装置に存在確認のパケットを送信し、応答がない場合にポートマッピングテーブルから外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置であり、予期しないエラーや端末自体の電源が切られたり、事故で正常に終了せずにポートが開いたままの状態を終了している場合等にも確実にポートを閉じることができる。この場合はタイマ手段によってカウントアウトするまでポートは使われることなく開いているのを防止できる。

【0018】

本発明の請求項5は、第1ネットワークと第2ネットワークとの間の通信パケットの中継を行う中継装置であって、第1ネットワーク側の外部ポート番号が第2ネットワーク側に接続された端末装置の内部IPアドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、外部ポート番号を指定した通信パケットを受信すると、ポートマッピングテーブルに基づいて内部ポート番号に変換して第2ネットワークに転送する制御手段と、第2ネットワーク側に接続された端末装置に存在確認のパケットを定期的を送信するための時間を計時するタイマ手段と、タイマ手段が計時した時刻に第2ネットワークに接続された端末装置に存在確認のパケットを送信し、応答がない場合にポートマッピングテーブルから外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置であり、一定時間間隔ごとに存在確認パケットを送信して端末の存在を確認するから、アクセスの有無と関係なくポートの使用未使用をチェックすることができ、予期しないエラーや端末自体の電源が切られたり、事故で正常に終了することがなく、ポートが開いたままの状態を終了している場合等にも確実にポートを閉じることができる。この場合はタイマ手段によってカウントアウトするまでポートは使われることなく開いているのを防止できる。

【0019】

本発明の請求項6は、ポート管理手段が、第2ネットワークに接続された端末

からの要求に基づいてポートマッピングテーブルへの登録を行うことを特徴とする請求項1～5のいずれかに記載の中継装置であり、第2ネットワークに接続したり電源をONしたときに、中継装置の存在を通知するパケットを端末は受信するとポートマッピングの登録が可能であることを知り必要なポートマッピングを中継装置に向けて要求を送信し、これを受信した中継装置のポート管理手段がポートマッピングテーブルへの登録して外部ポート番号を割り当て、ポートを開設できる。

【0020】

本発明の請求項7は、中継装置が、UPnP規格に従ってIPパケットを動的にポートフォワーディングするルータであることを特徴とする請求項1～6のいずれかに記載の中継装置であり、UPnP規格に従ったルータは、無期限だけでなく有期限でポートを割り当てることができるので、ベンダーによらず自動的に第1ネットワーク側の外部ポート番号を設定したり、割り当てを削除することができる。

【0021】

本発明の請求項8は、第1ネットワークと第2ネットワークとの間の通信パケットの中継を行う中継装置であって、第1ネットワーク側の外部ポート番号が第2ネットワーク側に接続された端末装置の内部IPアドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、外部ポート番号を指定した通信パケットを受信すると、ポートマッピングテーブルに基づいて内部ポート番号に変換して第2ネットワークに転送する制御手段と、DHCPリース期限に再リースをするか否かを確認し、端末装置からの再リース要求を受信するDHCPサーバ部と、端末装置からの再リース要求がなかった場合には、ポートマッピングテーブルから外部ポート番号に関する登録を削除するポート管理手段を備えたことを特徴とする中継装置であり、DHCP機能を利用してきわめて簡単にポートを閉鎖できる。

【0022】

(実施の形態1)

本発明の実施の形態1における中継装置について説明する。図1は本発明の実

施の形態 1 における中継装置配下のクライアント端末にアクセスするネットワークシステムの構成図、図 2 は本発明の実施の形態 1 における中継装置の構成図、図 3 は本発明の実施の形態 1 におけるクライアント端末の構成図、図 4 は本発明の実施の形態 1 におけるサーバの構成図、図 5 は本発明の実施の形態 1 におけるポートマッピングテーブルの説明図、図 6 は本発明の実施の形態 1 におけるポート割当のフローチャート、図 7 は本発明の実施の形態 1 におけるタイマによるポート割当を削除するときのフローチャート、図 8 は本発明の実施の形態 1 におけるアクセス後の存在確認によるポート割当を削除するときのフローチャート、図 9 は本発明の実施の形態 1 における定期的な存在確認によるポート割当を削除するときのフローチャート、図 10 は本発明の実施の形態 1 におけるポート割当からタイマによるポート削除までのシーケンスの説明図、図 11 は本発明の実施の形態 1 におけるポート割当からアクセス後の存在確認によるポート削除までのシーケンスの説明図である。

【0023】

図 1 において、1 は TCP/IP で通信する広域ネットワーク (WAN) の 1 つであるインターネット (本発明の第 1 ネットワーク)、2 はインターネット 1 と接続可能なインタフェースを有し、ローカルエリアネットワーク (本発明の第 2 ネットワーク、以下、LAN という) 側のポートを複数備えて配下の各端末装置、例えば後述する画像サーバ 3 a, 3 b, 3 c に対してルーティングする、とくに UPnP 規格に従って IP パケットを動的にポートフォワーディングするルータ (本発明の中継装置)、3 a, 3 b, 3 c は画像サーバである。4 はインターネット 1 に接続して画像サーバ 3 a, 3 b, 3 c にアクセスできる端末、5 はブラウザ機能を搭載したコンピュータ端末、6 はホスト名でアクセスするとグローバル IP アドレス (本発明の外部 IP アドレス、以下、外部 IP アドレスという) を応答する DNS (Domain Name System) サーバで、7 はインターネット 1 に接続されたウェブサーバある。8 は、LAN 内で所定のローカル IP アドレス (本発明の内部 IP アドレス、以下、IP アドレスという) の中から画像サーバ 3 a, 3 b, 3 c に IP アドレスを割り当てる DHCP (Dynamic Host Configuration Protocol) サ

サーバである。なお、DHCPサーバ8はルータ2に搭載するのもよい。

【0024】

実施の形態1においては、画像サーバ3a, 3b, 3cをルータ2に接続すると、各サーバはルータ2に外部ポートの割り当てを要求し、使用可能な外部ポート番号を登録する。例えば、実施の形態1の画像サーバ3a, 3b, 3cのうちの1台、例えば画像サーバ3aが外部ポート番号の割り当てを要求したときは、ルータ2は所定の外部ポート番号、例えば「80」を割り当てる。このとき、インターネット1側からこのポート番号「80」を有した画像サーバ3aを認識できることになり、インターネット1側からポート番号「80」でアクセスしたときは、ルータ2のポートフォワード機能により、画像サーバ3a, 3b, 3cのうちの1台である画像サーバ3aに通信パケットは確実に着信する。なお、ルータ2に登録されるポート番号には、インターネット1側で使用される外部ポート番号と、LAN側で使用される内部ポート番号があるが、UPnP規格に従ってルータ2に動的に割り当てようとする外部ポートが既に使用中の場合は別のポート番号を再度割り当てよう要求を出すことになる。

【0025】

同様に、他の2つの画像サーバ3b, 3cに対してルータ2は外部ポートの割り当て例えば「2000」「2001」の割り当て要求を行う。これによってインターネット1を介して端末4からユーザがこの外部ポート番号で画像サーバ3a, 3b, 3cにアクセスしたとき、画像サーバ3a, 3b, 3cへの接続が可能になるものである。

【0026】

次に、実施の形態1のルータ2の内部構成について図2に基づいて説明する。図2において、11は画像サーバ3a, 3b, 3cのインターネット1との間のグローバルネットワークI/F部、12₁, 12₂, ..., 12_nはそれぞれ画像サーバ3a, 3b, 3c, ...等に接続されるローカルネットワークI/F部である。複数のグローバルIPアドレスを有する場合には、グローバルネットワークI/F部11は複数設けられる。

【0027】

14は制御プログラムや各種データをメモリする記憶部であり、14aはポートマッピング情報を割り当てるためのポートマッピングテーブル、14bはポートを閉じるための設定時間を設定するための利用実績メモリ部である。このポートマッピングテーブル14aは外部IPアドレスと外部ポート番号をIPアドレスと内部ポート番号に関係付けるものである。なお、グローバルネットワークI/F部が一つの場合は、外部IPアドレスの関連付けは必ずしも必要ない。

【0028】

15は制御部であって、中央演算処理装置(CPU)に制御プログラムを読み込んで各機能を奏する機能実現手段として構成される。制御部15は、システム全体の制御を行うとともに、ポートマッピングテーブル14aに従ってアドレス変換を行い、受信したパケットをポートフォワーディングする。16は画像サーバ3a, 3b, 3c, ...のポート番号を割り当て、割り当てたポート番号を削除するポート管理手段であり、17はパケットが通過してからの時間をカウントするタイマ手段である。

【0029】

実施の形態1のルータ2は、画像サーバ3a, 3b, 3cやコンピュータ端末5からの外部ポート番号の無期限の割当て要求により、開いた外部ポートがセキュリティホールとならないように、時間を計る等により開きっぱなしのポートを閉じる。そのための第1の方法は、その外部ポートに対してアクセスがあったときから一定時間またはユーザが設定した時間が経過するとその外部ポートを閉じるもので、タイマ手段17は時間を計測して閉じるタイミングを検出するものである。第2の方法は、そのポートに対してアクセスがあってから所定の時間を経過すると、通信管理を実行する制御部15が、その外部ポートへのアクセスのフォワード先に対し、pingコマンドやARPコマンドを送信して存在確認を行い、存在しないことが判明した時点にポートを閉じる方法である。第3の方法は、ポート管理手段16がその外部ポートへのアクセスのフォワード先に対して定期的にpingコマンドやARPコマンドを送信してLAN内の端末装置の存在確認を行い、存在しないことが判明した時点にポートを閉じるものである。そして、第4の方法は、ポート割当て要求を受信してポートを開き、その後DHCPリ

ースの期限が経過したとき再リースの要求がないときポートを閉鎖するものである。詳細は後で説明する。

【0 0 3 0】

次に、実施の形態 1 の画像サーバ 3 a, 3 b, 3 c の内部構成について図 3 に基づいて説明する。図 3 において、2 1 は画像サーバ 3 a, 3 b, 3 c のインターネット 1 との間のネットワークインタフェースであり、端末 4 のブラウザからのリクエストを画像サーバ 3 a, 3 b, 3 c に伝え、画像サーバ 3 a, 3 b, 3 c からのウェブページを表示するために HTML 等のマークアップ言語で記述されたデータやカメラ部 2 2 で撮像した画像をインターネット 1 に送信する。2 2 はカメラ部、2 3 はカメラ部 2 2 に設けられた CCD あるいは CMOS 撮像素子等からの映像信号である R, G, B 信号あるいは補色信号を処理し、輝度信号 Y と色差信号 C r, C b 信号を発生して J P E G 形式、M P E G 形式その他の圧縮形式に圧縮する画像データ生成部である。

【0 0 3 1】

2 4 は制御プログラムや各種データをメモリする記憶部であり、2 4 a は HTML 等のマークアップ言語により表示指示やリンク情報が記述された複数のファイルを記憶している HTML 記憶部、2 4 b は画像データ生成部 2 3 で圧縮した画像データを格納する画像記憶部である。

【0 0 3 2】

2 5 は、プロトコル T C P / I P でインターネット 1 との通信を行うウェブサーバ部であり、2 6 は、端末 4 のブラウザからウェブサーバ部 2 5 にアクセスがあったときに、ブラウザに対して HTML 等で構成されたファイルを記憶部 2 4 から取り出して、状況に応じて動的に HTML 等を生成し直し、送信する HTML 生成部である。2 7 は制御部であって、中央演算処理装置 (C P U) に制御プログラムを読み込んで各機能を奏する機能実現手段として構成される。2 8 はカメラ部 2 2 のパンチルト等の操作を行うモータ等から構成される駆動部、2 9 は駆動部 2 8 を駆動させるカメラ制御部である。制御部 2 7 は、ブラウザからの要求を処理し HTML 生成部 2 6 を動作させてウェブページ用ファイルを生成したり、ブラウザへ送信する画像データを記憶部から取り出したり、さらにカメラ制

御部 29 に対してモードを指定して動作させるものである。

【0033】

続いて、端末 4 の内部構成について図 4 に基づいて説明する。31 は端末 4 のインターネット 1 との間のネットワークインタフェースであり、画像のリクエストを画像サーバ 3a, 3b, 3c に伝え、ウェブページを表示するための HTML 等のマークアップ言語で記述されたテキストデータや画像データをインターネット 1 から受信する。32 はディスプレイに表示を行う表示手段、33 は表示手段 32 によって受信したウェブページを表示し、GUI により画面上表示した制御ボタンやアイコン等で画像のリクエストを行うブラウザ手段である。

【0034】

34 は制御プログラムや各種データをメモリする記憶部、35 はキーボードやマウス等の入力手段、36 は音声データを再生することができる音声出力手段である。音声出力手段 36 は圧縮されたデータを伸長して再生する。なお、音声出力手段 36 はインターネット 1 を介して受信したプラグインソフトでもよい。37 は制御部であって、中央演算処理装置 (CPU) に制御プログラムを読み込んで各機能を奏する機能実現手段として構成される。

【0035】

さて、実施の形態 1 のルータ 2 において、UPnP フォーラムの規格によって動的にポートフォワーディング設定を行うときの動作の説明を図 6 に基づいて行う。ルータ 2 は、画像サーバ 3a, 3b, 3c が接続されたり、電源を ON したり、コンピュータ端末 5 のアプリケーションが始動したとき、画像サーバ 3a, 3b, 3c やコンピュータ端末 5 からポート割当て要求を受信すると、ポート管理手段 16 がポートの割当てを行い、ポートマッピングテーブル 14a に登録する。

【0036】

まず、ルータ 2 の制御部 15 はポート割当て要求パケットを受信するまで待機し、ポート割当て要求があるか否かをチェックする (step 1)。制御部 15 は、ポート割当て要求がないときは再び待機し、ポート割当て要求があった場合にはポート割当てが可能か否かがチェックする (step 2)。ポート割当てが可能である場

合、制御部 15 は、ポートを割り当てて応答し (step 3)、ポートマッピングテーブル 14 a に登録する (step 4)。step 2 においてポート割当ができない場合には、制御部 15 は、ポート割当不可応答を行い (step 5)、step 1 に戻って待機する。

【0037】

このとき、外部のポート番号とともにポートマッピングテーブル 14 a に登録する内部のポート番号及び内部の IP アドレスは、ポート割当要求パケットの中に記載されているが、ポート割当要求の TCP/IP ヘッダ領域から取り込むことも可能である。

【0038】

ポートマッピングテーブル 14 a には、LAN 内の内部ポート番号とインターネット 1 側の外部ポート番号のほかに、画像サーバ 3 a, 3 b, 3 c の IP アドレス、ホスト名、最後のアクセスがあつてからポートを閉じるための設定時間が登録される。この IP アドレスは、画像サーバ 3 a, 3 b, 3 c が DHCP サーバ 8 に対して DHCP 発見パケットを送信し、DHCP サーバ 8 が与えたものである。そして、設定時間は画像サーバ 3 a, 3 b, 3 c の存在確認を行うためにパケットを送信するまでの時間であってもよい。さらに、存在確認を定期的に行うための ping または ARP を送信する時間間隔を登録しておくこともできる。

【0039】

図 5 はこのポートマッピングテーブル 14 a の具体例を示している。図 5 において、ホスト名「マシン 1」の画像サーバ 3 a は、LAN に接続されると、DHCP サーバ 8 によって IP アドレス「192.168.0.1」が割り当てられ、UPnP 規格のルータ 2 によって外部ポート番号「80」が割り当てられる。内部ポート番号「8080」は画像サーバ 3 a がポートフォワードのためのポート割当要求を行った内部ポート番号である。設定時間 10 分はデフォルト値であり、最終のパケットが通過してからポートを閉鎖するまでの時間である。

【0040】

同様にホスト名「マシン 2」に対しては、ルータ 2 の割り当てた外部ポート番

号「2000」、内部ポート番号「80」、DHCPサーバ8によって割り当てられたIPアドレス「192.168.0.3」が登録され、設定時間20分が設定されている。また、ホスト名「マシン3」に対しては、外部ポート番号「2003」、内部ポート番号「101」、IPアドレス「192.168.0.3」が割り当てられ、設定時間として5分が登録される。このホスト名「マシン2」と「マシン3」の関係は、同一IPアドレスを有しており、例えば、図1のコンピュータ端末5において複数のブラウザアプリケーション（ネットワークエクスプローラ等）を起動させて、起動したブラウザがそれぞれポート割当要求を行ったような場合である。コンピュータ端末5において複数のブラウザアプリケーションを起動させた場合、それぞれのブラウザには、外部との通信のために異なるポート番号が割当てられる（図5においては「80」、「101」）。このように本実施の形態1のルータ2は、設定時間が経過すると画像サーバ3a、3b、3cやコンピュータ端末5が登録した外部ポートは閉鎖される。

【0041】

ここで、図7に基づいて画像サーバ3a、3b、3cがポート割当を受けた後、タイマ手段17によるポート閉鎖処理について以下説明する。この処理は最終のアクセスがあった後一定時間が経過するとポートを閉じるものである。図7に示すように、ポート割当を行ったポートに対してポート管理手段16はカウントダウンするための時間をセットする時間フラグを設定する（step11）。さらにタイマ手段17により一定時間のカウントを始める。次いでポートフォワードのアクセスがあったか否かがチェックされる（step12）。step12において、アクセスがあった場合には該ポートの時間フラグを更新する（step13）。step12においてアクセスがない場合、現時刻と時間フラグの時間とを比較し（step15）、比較した時刻が所定時間を超えているか否かがチェックされ（step16）、所定時間を超えていない場合はstep12に戻り、越えた場合はstep18に進む。なお、step13で時間フラグが更新されるのは、step15、step16のプロセスを経るため、一定時間が未経過でアクセスがあった場合である。

【0042】

s t e p 1 3 において、時間フラグを更新した後、ポートフォワードが可能かどうかチェックされ (s t e p 1 4) 、可能であればパケットをこのポートにフォワーディングして (s t e p 1 7) 、 s t e p 1 2 に戻る。 s t e p 1 4 でポートフォワードができない場合と、 s t e p 1 6 で所定の時間を超えている場合、該当するポートのポート番号をポートマッピングテーブル 1 4 a から削除する (s t e p 1 8) 。次いで、ルータ 2 は画像サーバ 3 a , 3 b , 3 c に対してポート割当強制削除通知を送信して (s t e p 1 9) 、終了する。なお、 s t e p 1 4 において、ポートフォワーディングが不可の場合、直ちに s t e p 1 8 に進むのではなくて、複数回連続して不可の状態が続いた場合だけ進むようにしてもよい。複数回連続していないときは s t e p 1 2 に戻る。

【 0 0 4 3 】

ところで、以上はタイマ手段 1 7 が一定時間をカウントして処理を行ったが、この時間はユーザの利用実態と密接な関係がある。従って、上述したように常に一定時間をカウントするのではなく、ユーザの利用実態に沿った時間を設定してポートを閉鎖するのも好適である。この場合、制御部 1 5 は画像サーバ 3 a , 3 b , 3 c ごと (ユーザごと) の利用実績、すなわちポートを開いてから閉鎖するまでの過去の実績の最大時間を記録しておき、その 1 1 0 % の値を閉鎖時間として使用するものである。利用されているかどうか、利用実績の判断はポート開放要求またはパケットの通過実績の有無をモニタすることで行う。ユーザ自身が希望で任意に設定してもよい。

【 0 0 4 4 】

また、上述の説明においては、インターネットから外部ポートへ最終のポートフォワードのアクセスがあった後一定時間が経過するとポートを閉じることとしたが、外部ポートからの最終のポートフォワードのアクセスに加えて、登録された外部ポート番号からインターネットへ送信されていく最後の通信パケットを考慮に入れてポートを閉じることとしてもよい。

【 0 0 4 5 】

このように、本実施の形態 1 のルータ 2 は、UP n P 規格の動的に開かれたポートを自動的に閉じるためのタイマ手段 1 7 を備えているから、ポート開設され

てから所定時間経過した後ポートを閉じることができる。さらに、ユーザが自分にとって任意の最適時間を設定できるので、もっともユーザにとって好ましい時間を設定できる。また、ポートを開いて閉じるまでの利用実態に沿うように、過去の利用の中で最大時間を記憶するので、次の要求に対しては前回利用時間より大きい時間を設定すれば、利用中にも関わらずポートを閉鎖することはない。

【0046】

次に、図8に基づいて画像サーバ3a, 3b, 3cがポート割当を受けた後、存在確認によって行うポート閉鎖処理について説明する。この処理は画像サーバ3a, 3b, 3cがLAN内に存在しないことが確認されるとポートを閉じるものである。図8に示すように、ポート割当を行ったポートに対してポート管理手段16は時間フラグを設定する(step 21)。そしてタイマ手段17は一定時間のカウントを始める。次いでポートフォワードのアクセスがあったか否かがチェックされる(step 22)。step 22において、アクセスがあった場合には時間フラグを更新する(step 23)。step 22においてアクセスがない場合、現時刻と時間フラグの時間とを比較し(step 25)、比較した時刻が所定時間を超えているか否かがチェックされ(step 26)、所定時間を超えていない場合はstep 22に戻り、所定時間が経過している場合は以下説明するpingコマンドやARPコマンド等の存在確認パケットを送信し(step 28)、応答があるか否かをチェックする(step 29)。なお、step 23で時間フラグが更新されるのは、step 25, step 26のプロセスを経るため、一定時間が未経過でアクセスがあった場合である。

【0047】

ところで、この存在確認を行うpingコマンドは端末間の通信確認をするためのネットワークコマンドであり、データパケットの送受信が成功したか否かの確認等を行うものである。このコマンドを受信した端末装置はこれを実行することで「ICMPメッセージ」を送出する。「ICMPメッセージ」を受信することによって通信確認が行え、相手端末の存在も確認できるものである。

【0048】

また、ARP (Address Resolution Protocol)

は、IPアドレスからMACアドレスを知るために使われるプロトコルである。MS-DOSなどではARPコマンドを使うことによって、MACアドレスを格納しているARPキャッシュテーブルの設定に問題がないかを確認することができる。LAN内にMACアドレスを知りたいIPアドレスを含んだARPパケットを送信すれば、該当するIPアドレスを持つ端末が応答するので、該当マシンのMACアドレスを知ることができる。ARPパケットはpingでは応答しない端末（ファイアウォール）を搭載した機器などに対しても有効である。

【0049】

続いて、step 23において、時間フラグを更新した後、ポートフォワードが可能かどうかチェックされ（step 24）、可能であればパケットをこのポートにフォワーディングして（step 27）、step 22に戻る。step 24でポートフォワードができない場合と、step 29で応答がなかった場合、該当するポートのポート番号をポートマッピングテーブル14aから削除して（step 30）、終了する。step 29で応答があった場合もそのまま終了する。なお、step 24において、ポートフォワーディングが不可の場合、直ちにstep 30に進むのではなくて、複数回連続して不可の状態が続いた場合だけ進むようにしてもよい。複数回連続していないときはstep 22に戻る。

【0050】

次に、図9に基づいて画像サーバ3a、3b、3cがポート割当を受けた後、ルータ2が定期的に行う存在確認パケットによってポート閉鎖処理について説明する。図9に示すように、タイマ手段17は定期的にpingまたはARPを送信する間隔の一定時間をカウントする。所定時間が経過するまでカウントされ、カウントアウトすると（step 41）、ルータ2はpingコマンドやARPコマンド等の存在確認パケットを送信し（step 42）、応答があるか否かをチェックする（step 43）。

【0051】

続いて、step 43において応答がなかった場合、該当するポートのポート番号をポートマッピングテーブル14aから削除して（step 44）、終了す

る。step 43で応答があった場合もそのまま終了する。

【0052】

このように一定時間間隔、例えば10分ごとにpingコマンドやARPコマンド等の存在確認パケットを送信して端末の存在を確認するから、ネットワークを介してのアクセスの有無と関係なくポートの使用未使用をチェックすることができ、予期しないエラーや端末自体の電源が切られたり、事故で正常に終了せずポートが開いたまま終了しているような場合にも確実にポートを閉じることができる。上述の2つの方法と異なり、タイマ手段17がカウントアウトするまではポートが放置されるといったことがない。

【0053】

続いて、LAN内のローカルサーバであるコンピュータ端末5のアプリケーションA（例えば、ブラウザアプリケーション）が、インターネット1に接続されたグローバルサーバであるウェブサーバ7にアクセスし、タイマ手段17によって割当ポートを削除する場合のシーケンスについて説明する。図10に示すように、コンピュータ端末5が起動すると、DHCP発見パケットを送信してDHCPサーバ8からの応答を受け取り、IPアドレス「192.168.0.1」を割り当てられる。ここでコンピュータ端末5はDHCPサーバ8を使わず、静的に「192.168.0.1」をユーザが手動で割り付けてもよい。続いてコンピュータ端末5上で起動したアプリケーションAにはポート番号を「8080」がコンピュータ端末5上で割り当てられる。

【0054】

続いてアプリケーションAはルータ発見パケットを送信し（sq1）、ルータ2がこれに対して応答する（sq2）。これを受信するとアプリケーション5aはポート登録要求を送信し（sq3）、ルータ2はポート割当応答を行う。このポート登録要求にはルータ2の外部ポート番号「80」とアプリケーションAが使用するポート番号「8080」及びIPアドレス「192.168.0.1」が関連付けられており、ルータ2内でも関連付けられた状態で記録される。

【0055】

インターネット1側の機器から通信開始のパケットを受信するようなアプリケ

ーションBは、通常サーバアプリケーションであり、例えばウェブサーバなどである。この場合、インターネット上のグローバルIPアドレス「232.0.0.2」を持つウェブサーバ7から、ルータ2配下にあるコンピュータ端末5上のアプリケーションBに接続する際は「http232.0.0.1:80」でアクセスし(sq5)、ルータ2はこれをフォーワーディングルールに従って「http//:192.168.0.1:8080」へフォーワーディングを行う(sq6)。フォーワーディングされたパケットを受信したアプリケーションBは、レスポンスパケットをウェブサーバ7へ返す(sq7)。その後、コンピュータ端末5が事故などでインターネット上から消えた場合、ウェブサーバ7からのアクセスで(sq8)、要求パケットがコンピュータ端末5へフォーワーディング(sq9)されても、レスポンスパケットは送信されず、これが外部ポート「80」を使った最後の通信となる。

【0056】

ルータ2はパケットが登録ポートを通過した時点でタイマ手段17を毎回更新し、ポートフォーワーディングを継続するが、sq9でパケットが通過した後は更新されることがないため、やがてタイムアウトする。このように所定の時間が経過してもパケットが着信せずタイムアウトした場合、ルータ2はポート割当強制削除通知を画像サーバ3aに送信し(sq10)、ポート番号「80」をポートマッピングテーブル14aから削除する。

【0057】

同様に、コンピュータ端末5のアプリケーションB（例えば、ウェブサーバアプリケーション）へインターネット1に接続されたウェブサーバ7からアクセスがあり、コンピュータ端末5やアプリケーションBの存在確認によってルータ2が割当ポートを削除する場合のシーケンスについて説明する。以下説明するsq21～30は、上述のタイマ手段17で処理する場合のsq1～sq10と基本的に同一である。

【0058】

コンピュータ端末5が起動すると、DHCP発見パケットを送信してDHCPサーバ8からの応答を受け取り、IPアドレス「192.168.0.1」を割

り当てられる。ここでコンピュータ端末5はDHCPサーバ8を使わず、静的に「192.168.0.1」をユーザが手動で割り付けてもよい。続いてコンピュータ端末5上で起動したアプリケーション5aはポート番号を「8080」がコンピュータ端末5上で割り当てられる。

【0059】

続いてアプリケーションBはルータ発見パケットを送信し（sq21）、ルータ2がこれに対して応答する（sq22）。これを受信するとアプリケーションBはポート登録要求を送信し（sq23）、ルータ2はポート割当応答を行う（sq24）。このポート登録要求にはルータ2の外部ポート番号「80」とアプリケーションBが使用するポート番号「8080」及びIPアドレス「192.168.0.1」が関連付けられており、ルータ2内でも関連づけられた状態で記録される。

【0060】

その後、インターネット上のグローバルIPアドレス「232.0.0.2」を持つウェブサーバ7から、ルータ配下にあるコンピュータ端末5上のアプリケーションBに接続する際は「http232.0.0.1:80」でアクセスし（sq25）、ルータ2はこれをフォーワーディングルールに従って「http//:192.168.0.1:8080」へフォーワーディングを行う（sq26）。フォーワーディングされたパケットを受信したアプリケーションBは、レスポンスパケットをウェブサーバ7へ返す（sq27）。その後、コンピュータ端末5が電源断などでインターネット上から消えた場合、ウェブサーバ7からのアクセスで（sq28）、要求パケットがコンピュータ端末5へフォーワーディング（sq29）されても、レスポンスパケットは送信されず、これが外部ポート「80」を使った最後の通信となる。

【0061】

sq29でレスポンスのパケットが通過すると、ルータ2はタイマ手段17により所定の時間が経過するまでカウントする。この時間内に次のパケットが着信すればルータ2はポートを更新し、ポートフォーワーディングを続けるが、所定の時間が経過してもパケットが着信しなかった場合、ルータ2はアプリケーション

Bまたはコンピュータ端末5の存在確認を行う（s q 3 0）。

【0 0 6 2】

存在確認パケットに対して応答がなければ、外部ポート番号「8 0」と関連する事項をポートマッピングテーブル1 4 aから削除し、存在確認パケットに対して応答があった場合、ルータ2はポート割当強制削除通知を画像サーバ3 aに送信し（s q 1 1）、外部ポート番号「8 0」と関連する事項をポートマッピングテーブル1 4 aから削除する。

【0 0 6 3】

p i n g コマンドやA R P コマンド等の存在確認パケットを送信してアプリケーションBまたはコンピュータ端末5の存在を確認するから、予期しないエラーや端末自体の電源が切られたり、事故で正常に終了せずにポートが開いたままの状態を終了している場合等にも確実にポートを閉じることができる。この場合はタイマ手段によってタイムアウトするまでポートは使われることなく開いているのを防止できる。

【0 0 6 4】

最後に、図示はしないが、ポート割当要求を受信してポートを開き、その後D H C P に対する再リースの要求がないとき、ポートを閉鎖する場合について説明する。従って、ルータ2がD H C P サーバ機能を備えているのが望ましい。

【0 0 6 5】

この実施の形態の場合、ルータ2はD H C P サーバ8の代わりにD H C P サーバ部（図示しない）を搭載し、L A N 内の画像サーバ3 a，3 b，3 c やコンピュータ端末5等の端末のI P アドレスの割当を行うとともに、D H C P 機能を利用し、これらの端末がL A N 内に不存在であることを、D H C P リースの期限切れに行われる端末からの再リース要求の有無で確認する。これによってポートを閉じるものである。

【0 0 6 6】

D H C P のプロトコルによればリース期限の設定が可能であるが、このときリース期限終了前に再リースをするか否かを確認することが規定されている。この実施の形態はこの規定を利用するもので、一旦ポート割当要求してポートが開か

れた端末が、D H C P リースの期限が切れても I P アドレスの更新をしないということがその端末が L A N 内に存在しなくなったことを意味する、と判断するものである。

【 0 0 6 7 】

このため、ルータ 2 の D H C P サーバ部は、D H C P リース期限が到来すると、再リースするかをこの端末に確認し、再リース要求がされない場合には、ポート管理手段 1 6 がポートマッピングテーブル 1 4 a を検索し、そのポート番号を削除することによりポートを閉鎖する。この場合、ルータ 2 の D H C P 機能を利用し、きわめて簡単にポートを閉鎖できる。

【 0 0 6 8 】

【発明の効果】

本発明の中継装置によれば、ポートの未使用時間が所定時間を超えたとき、ポート管理手段によってポートを閉鎖するから、ポートが開かれたままでは不正アクセスされる危険があるが、所定時間以上経過するとポートは閉鎖され、これによって端末装置内部の情報が漏れることはない。

【 0 0 6 9 】

定期的に存在確認パケットを送信して端末の存在を確認するから、アクセスの有無と関係なくポートの使用未使用をチェックすることができ、正常に終了することがなく、ポートが開いたままの状態を終了している場合等にも確実にポートを閉じることができる。中継装置の D H C P 機能を利用すればきわめて簡単にポートを閉鎖できる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態 1 における中継装置配下のクライアント端末にアクセスするネットワークシステムの構成図

【図 2】

本発明の実施の形態 1 における中継装置の構成図

【図 3】

本発明の実施の形態 1 におけるクライアント端末の構成図

【図 4】

本発明の実施の形態 1 におけるサーバの構成図

【図 5】

本発明の実施の形態 1 におけるポートマッピングテーブルの説明図

【図 6】

本発明の実施の形態 1 におけるポート割当のフローチャート

【図 7】

本発明の実施の形態 1 におけるタイマによるポート割当を削除するときのフローチャート

【図 8】

本発明の実施の形態 1 におけるアクセス後の存在確認によるポート割当を削除するときのフローチャート

【図 9】

本発明の実施の形態 1 における定期的な存在確認によるポート割当を削除するときのフローチャート

【図 1 0】

本発明の実施の形態 1 におけるポート割当からタイマによるポート削除までのシーケンスの説明図

【図 1 1】

本発明の実施の形態 1 におけるポート割当からアクセス後の存在確認によるポート削除までのシーケンスの説明図

【図 1 2】

従来の動的ポートフォワーディングにおけるポート割当からポート解除までのシーケンスチャート

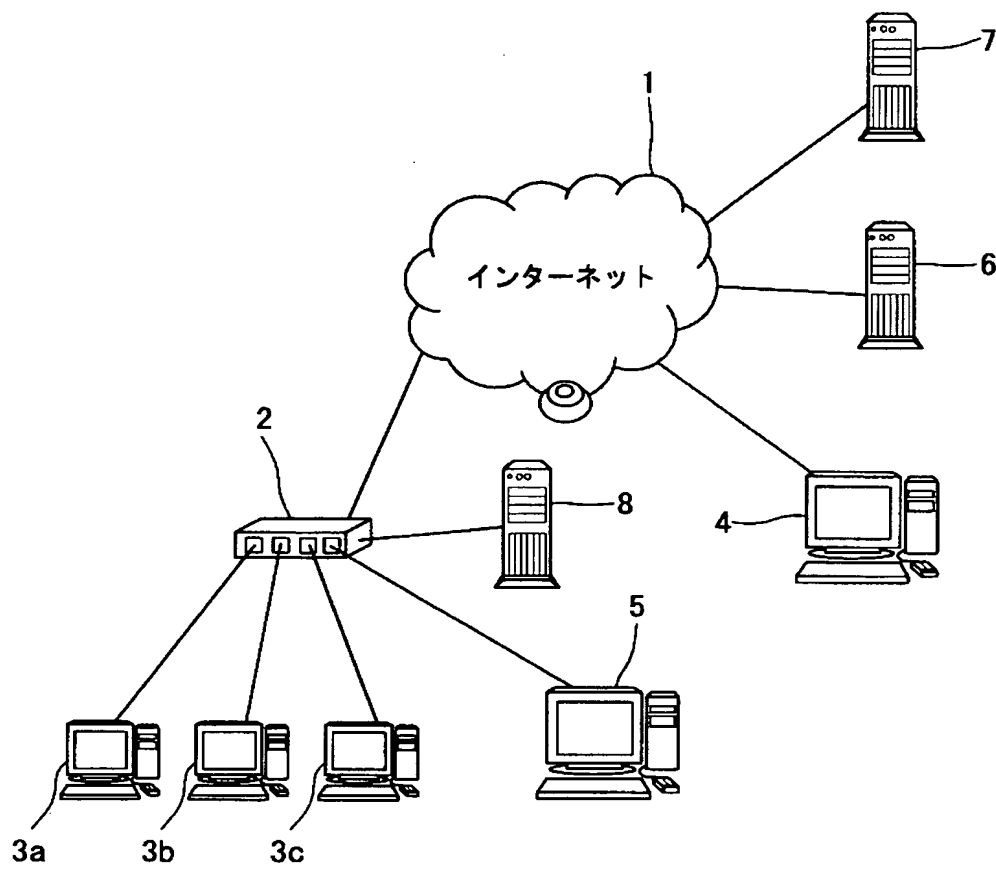
【符号の説明】

- 1 インターネット
- 2 ルータ
- 3 a, 3 b, 3 c 画像サーバ
- 4 端末

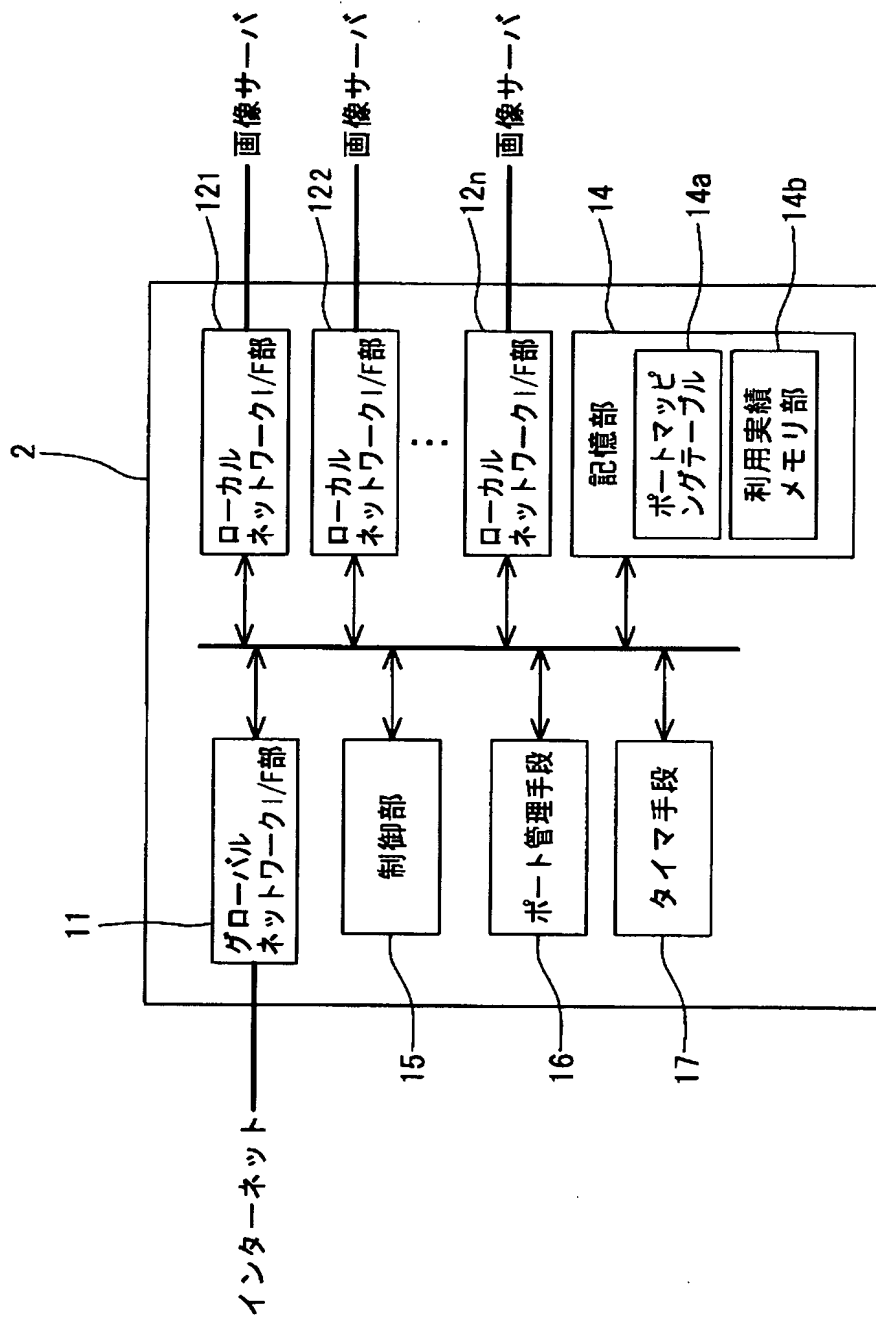
- 5 コンピュータ端末
- 6 DNSサーバ
- 7 ウェブサーバ
- 8 DHCPサーバ
- 11 グローバルネットワーク I/F部
- 12₁, 12₂, ..., 12_n ローカルネットワーク I/F部
- 14 記憶部
 - 14a ポートマッピングテーブル
 - 14b 利用実績メモリ部
- 15 制御部
- 16 ポート管理手段
- 17 タイマ手段
- 21 ネットワークインタフェース
- 22 カメラ部
- 23 画像データ生成部
- 24 記憶部
 - 24a HTML記憶部
 - 24b 画像記憶部
- 25 ウェブサーバ部
- 26 HTML生成部
- 27 制御部
- 28 駆動部
- 29 カメラ制御部
- 31 ネットワークインタフェース
- 32 表示手段
- 33 ブラウザ手段
- 34 記憶部
- 35 入力手段
- 36 音声出力手段

【書類名】 図面

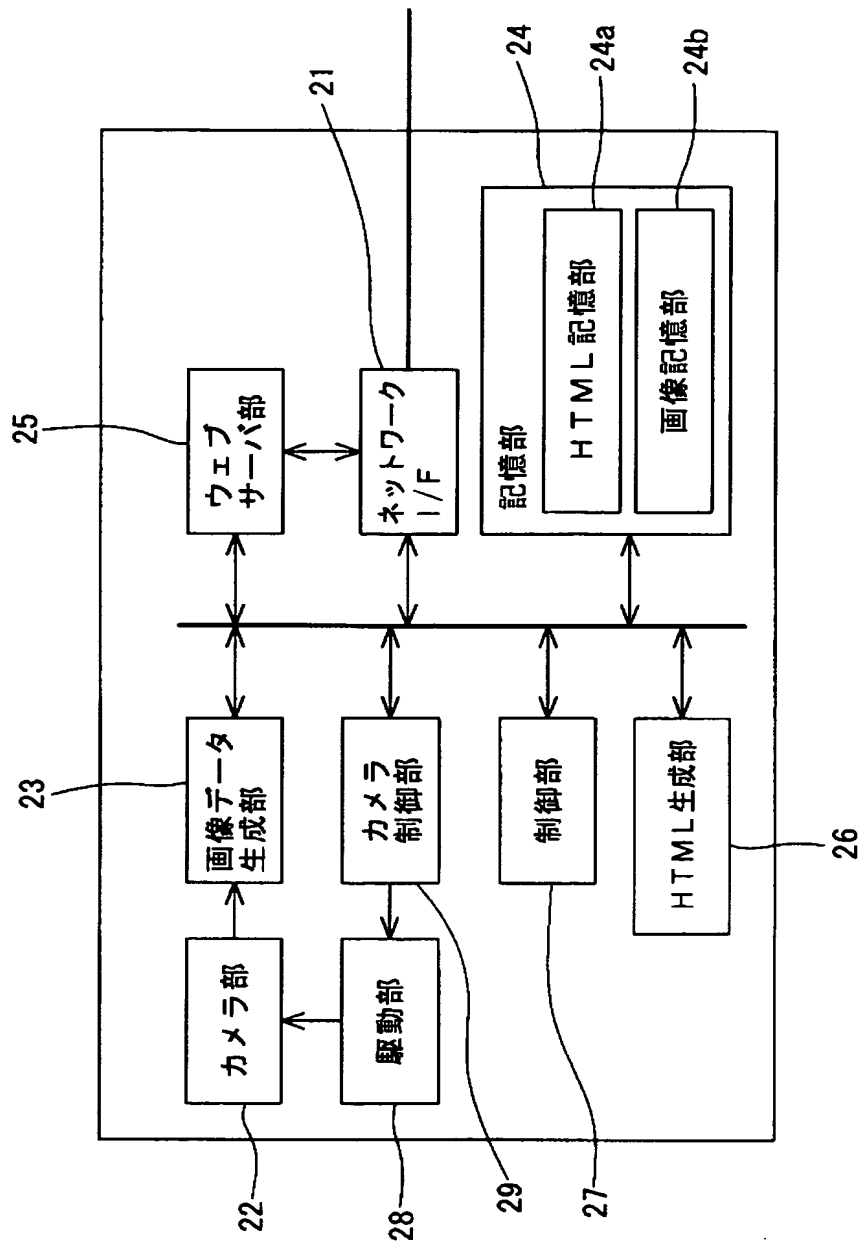
【図 1】



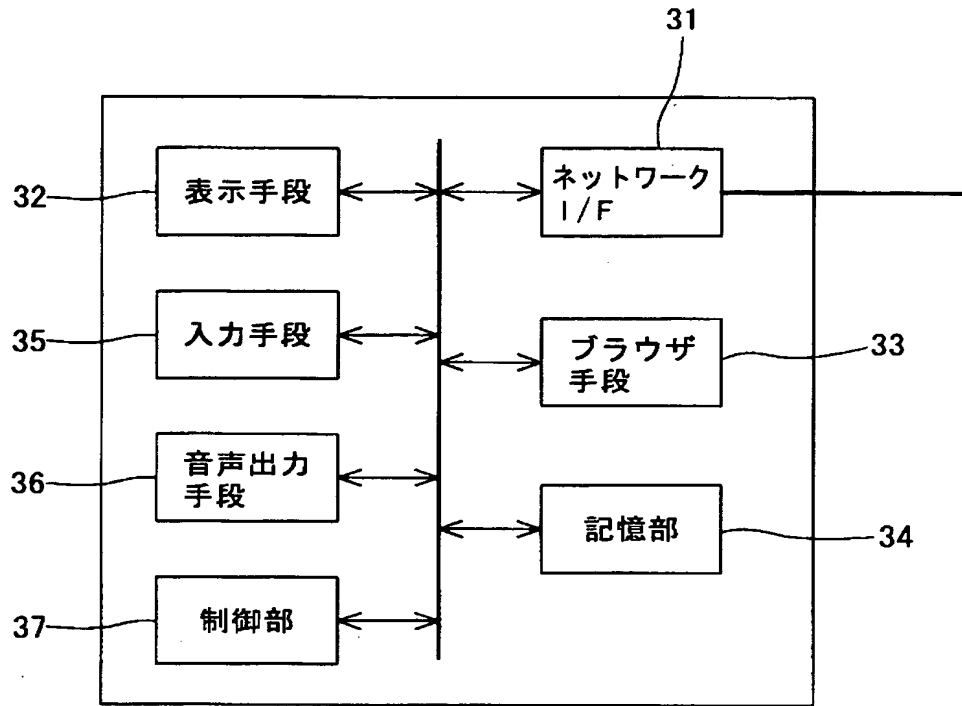
【図 2】



【図 3】



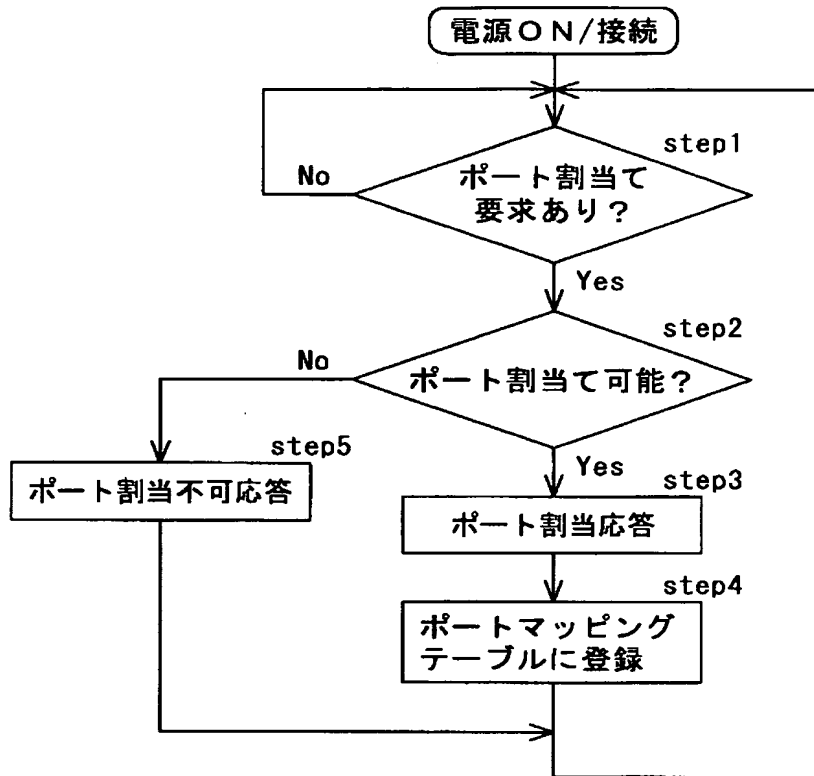
【図 4】



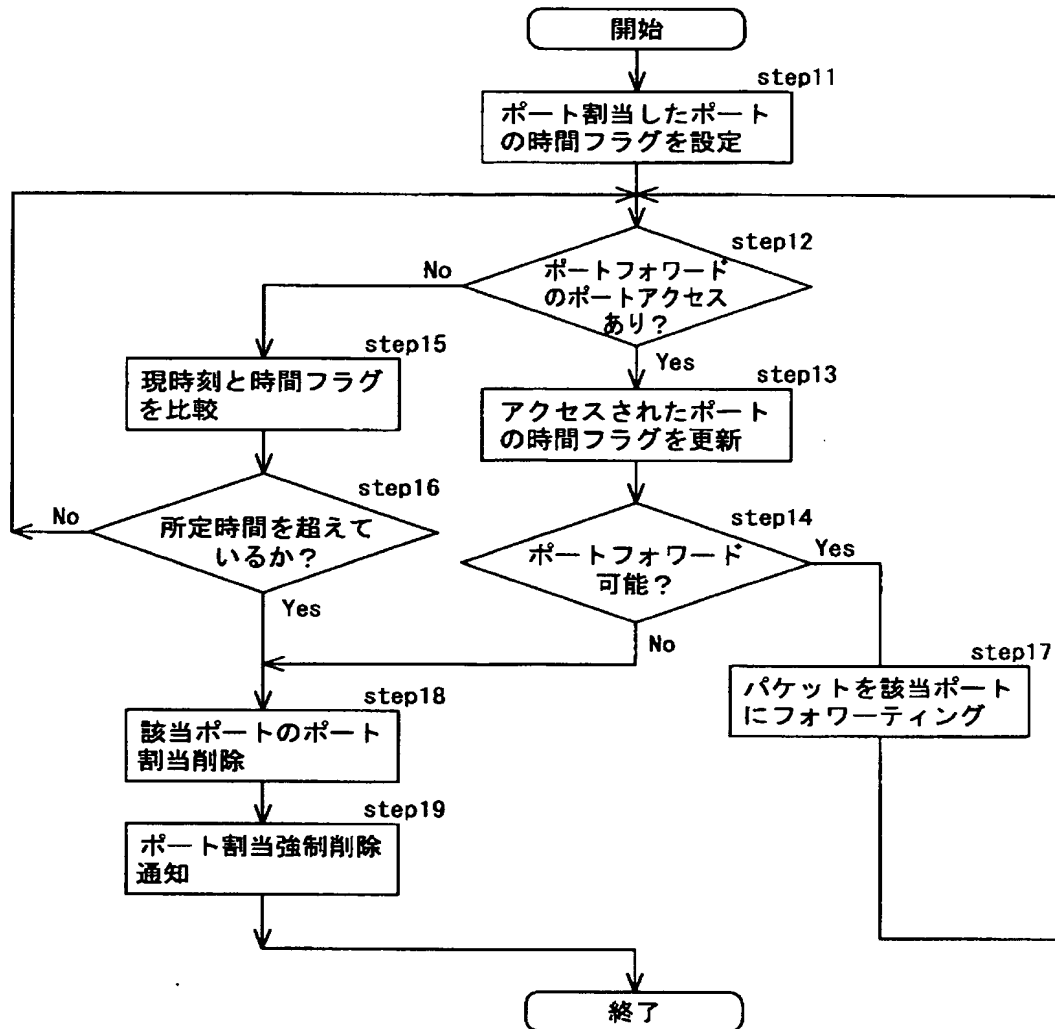
【図 5】

ルータ外側		ルータ内側			
外部ポート番号	外部IPアドレス	内部ポート番号	IPアドレス	ホスト名	設定時間
80	232.0.0.2	8080	192.168.0.1	マシン1	(10分)
2000		80	192.168.0.3	マシン2	20分
2003		101	192.168.0.3	マシン3	5分

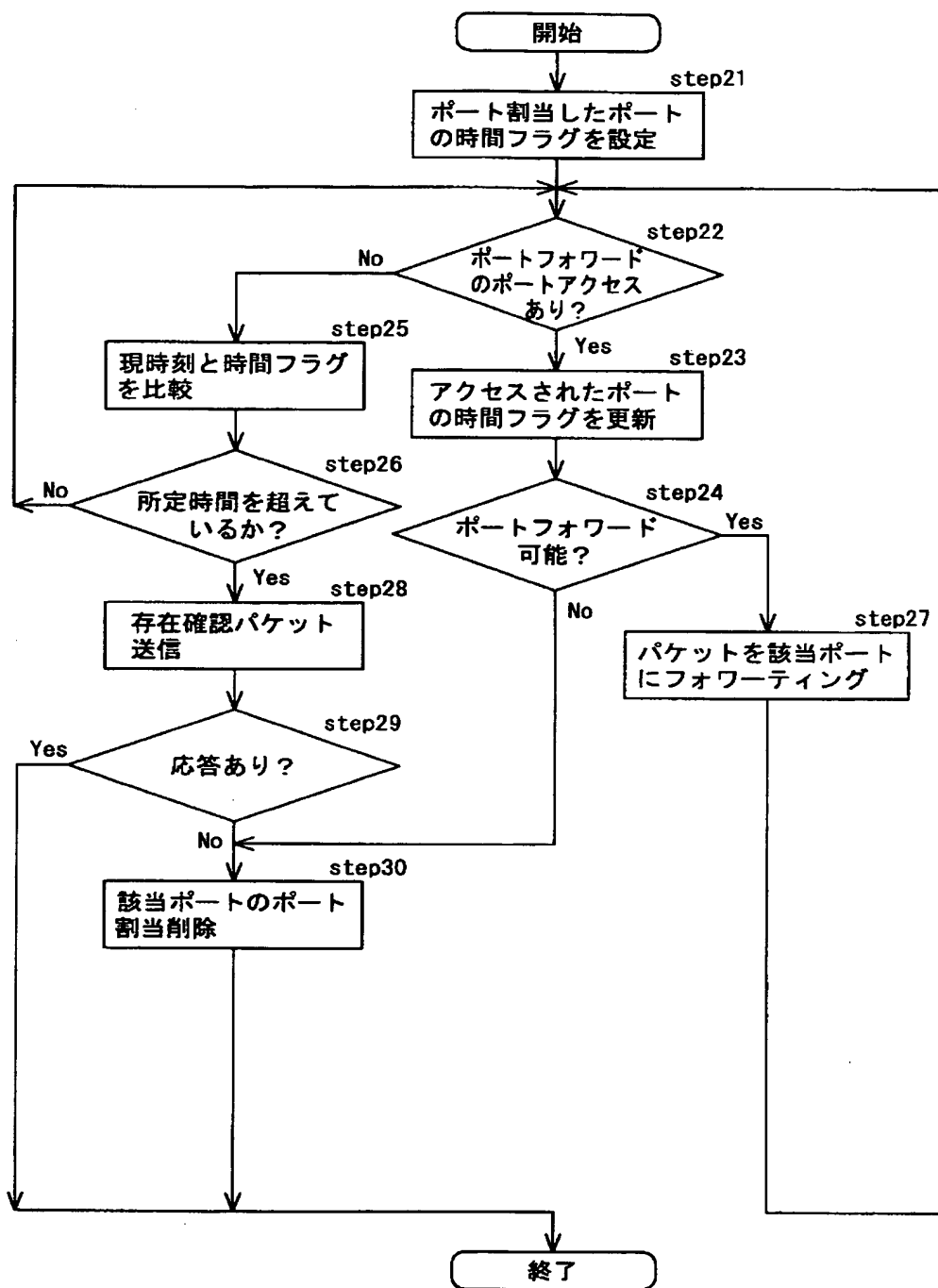
【図 6】



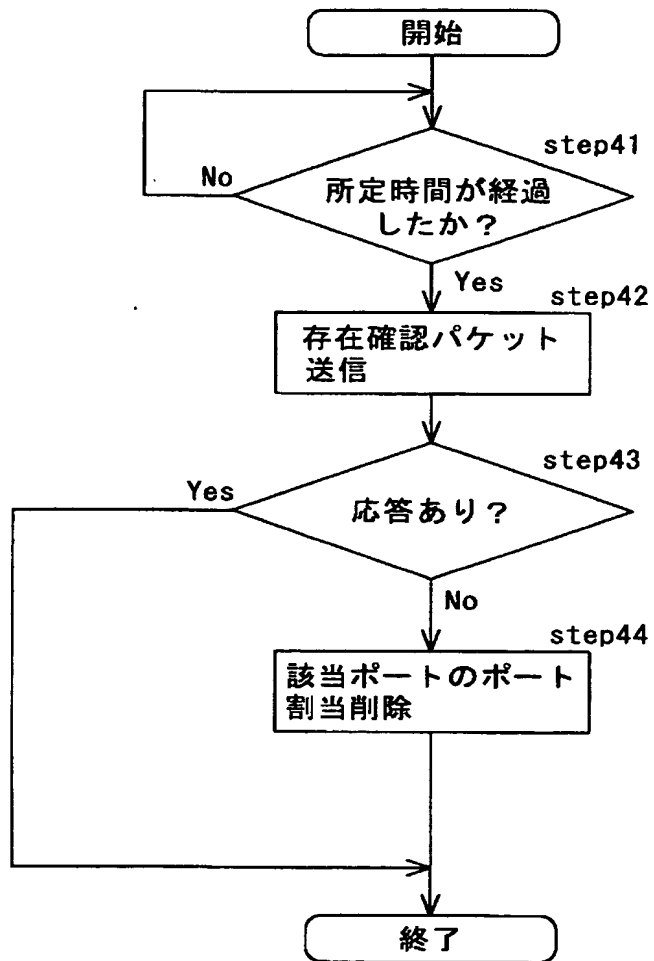
【図 7】



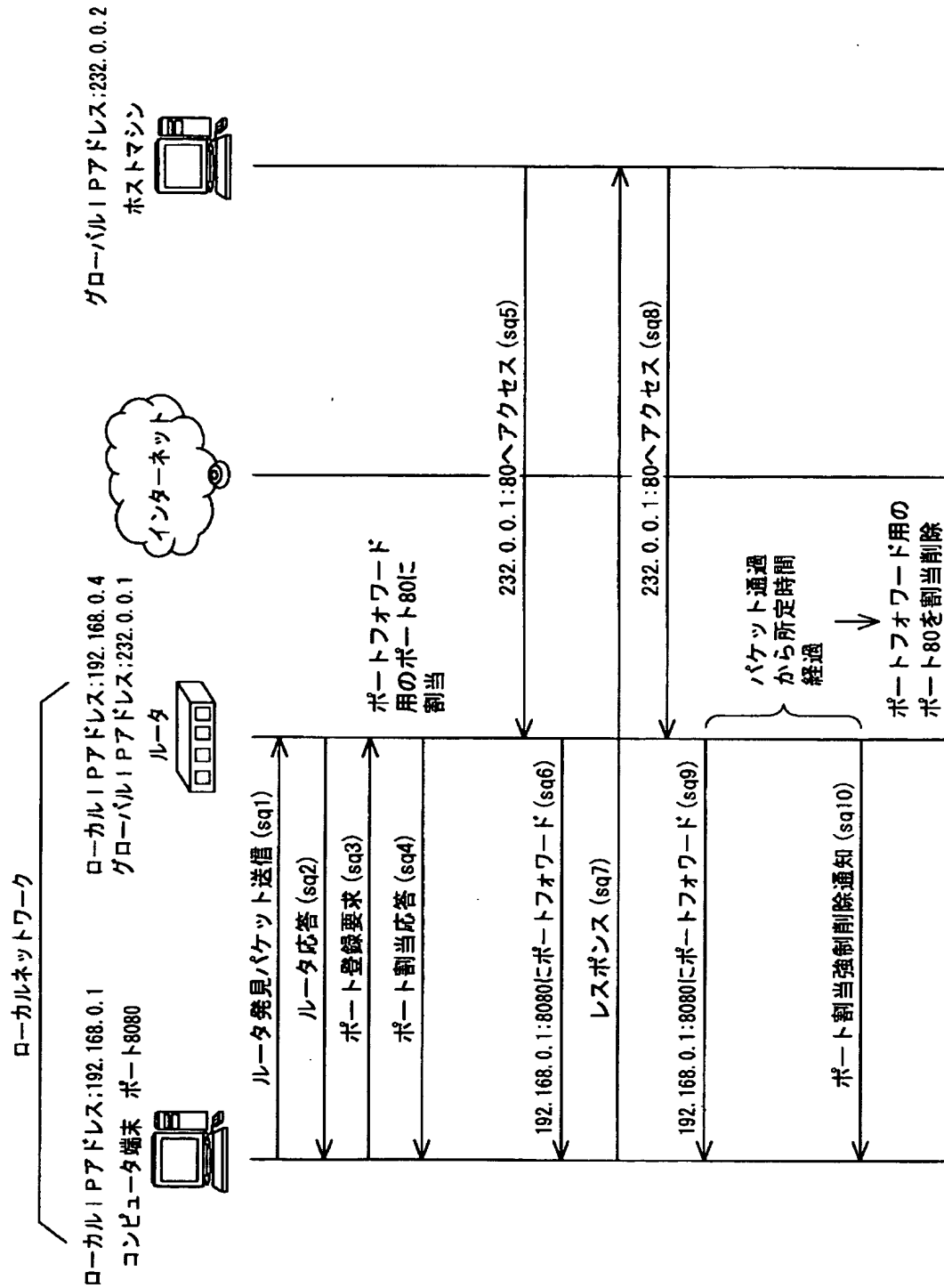
【図 8】



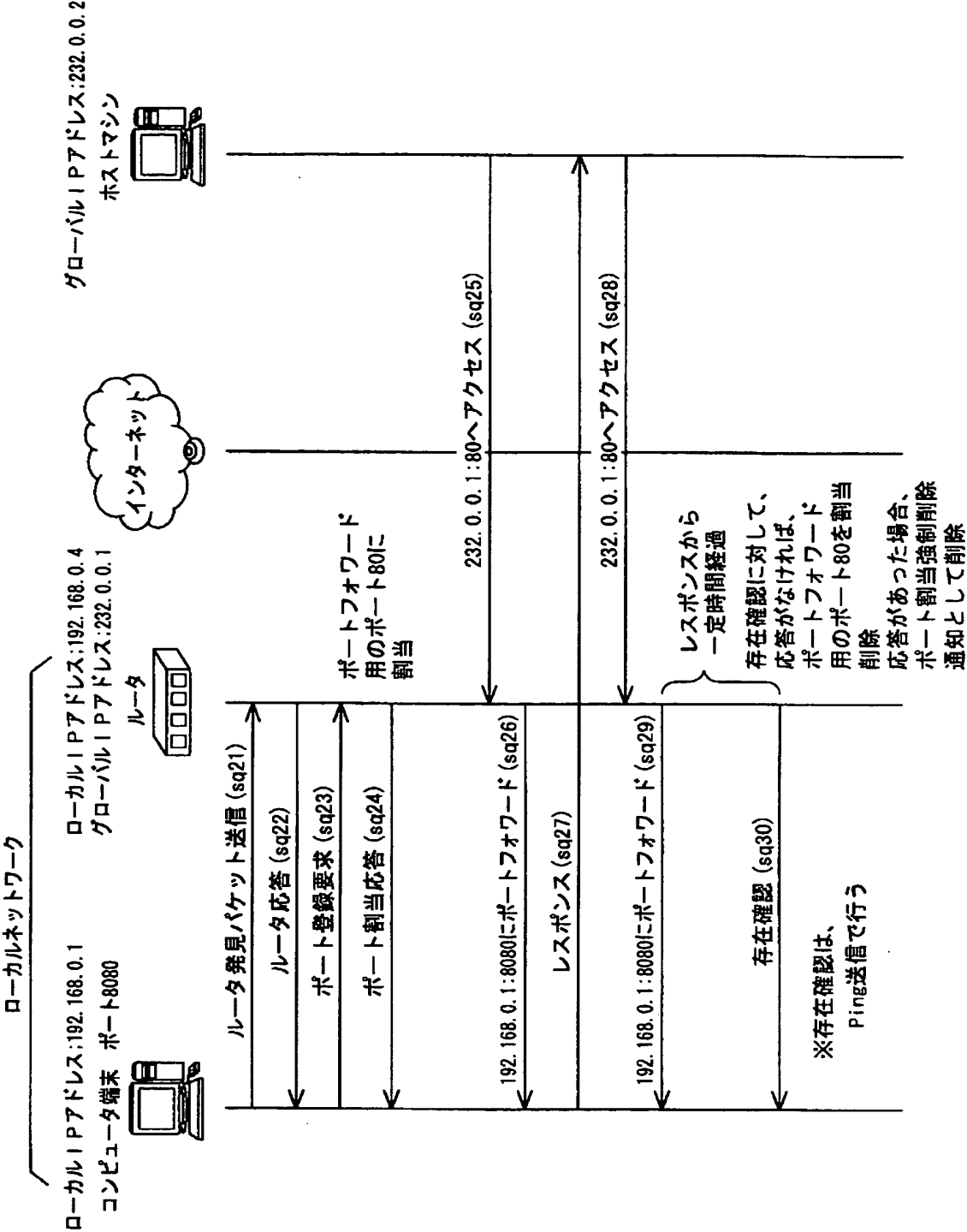
【図 9】



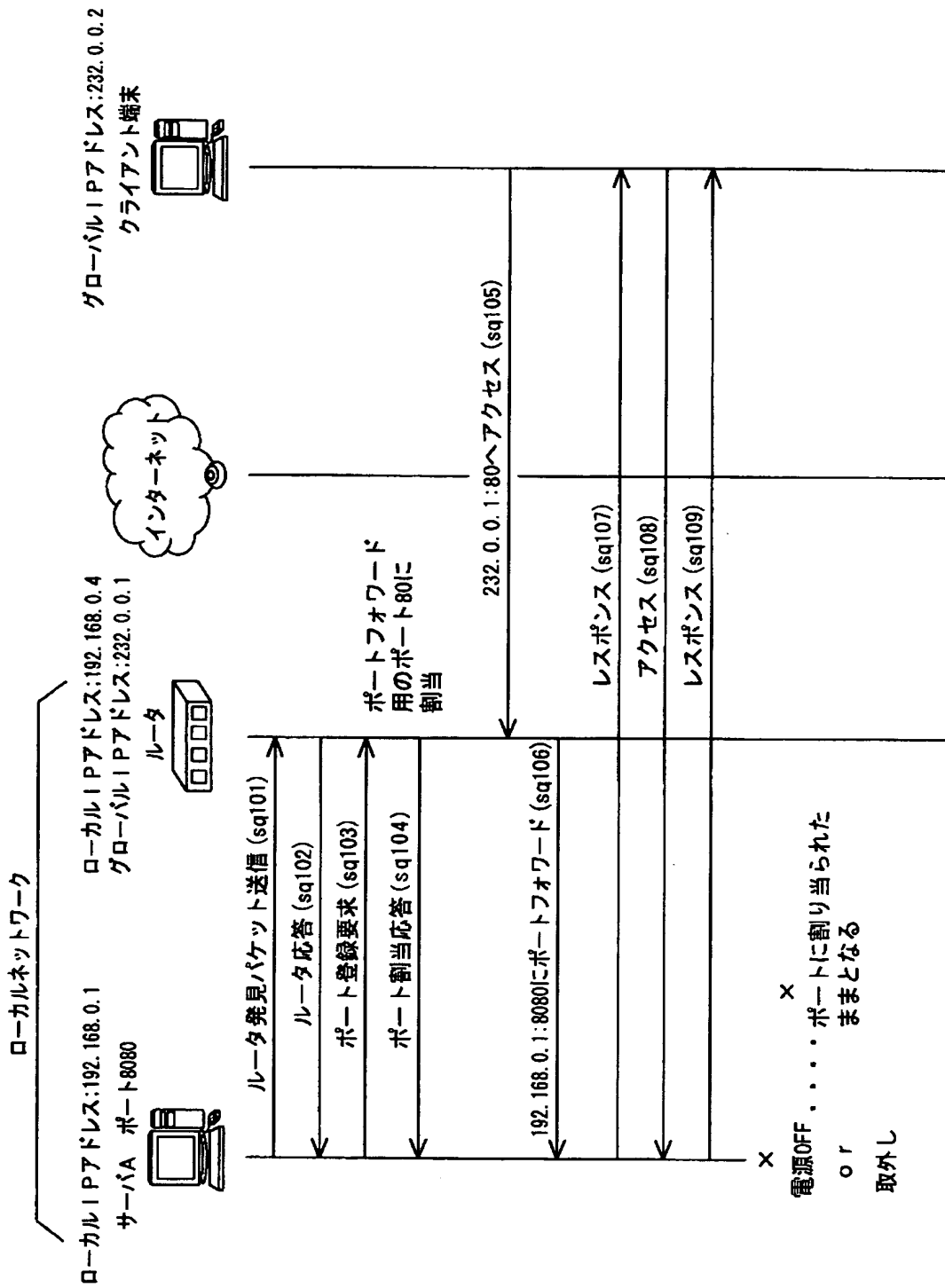
【図 10】



【図 11】



【図 12】



【書類名】 要約書

【要約】

【課題】 本発明は、動的に開かれたポートを設定に従って自動的に閉じる中継装置を提供することを目的とする。

【解決手段】 本発明は、インターネット側のグローバル I P アドレス及び外部ポート番号、または外部ポート番号が L A N 側に接続された端末装置のローカル I P アドレスと内部ポート番号に関係付けられたポートマッピングテーブルと、外部ポート番号を指定した通信パケットを受信すると、ポートマッピングテーブルに基づいて内部ポート番号に変換して L A N に転送する制御手段と、外部ポート番号を指定した通信パケットを転送してから該ポートの未使用時間を計時するタイマ手段と、ポートの未使用時間が所定時間になると登録マシンが L A N 上に存在するかどうかを確認して存在していない場合は、ポートマッピングテーブルから外部ポート番号に関する登録を削除するポート管理手段を備えたものである。

【選択図】 図 1

特願 2 0 0 3 - 1 1 5 5 6 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社